IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

TRACIE WILSON, on behalf of herself individually and on behalf of all others similarly situated, Plaintiff, v. HARVARD PILGRIM HEALTH CARE, INC. and POINT32HEALTH, INC., Defendants.	Case No. 1:23-cv-11288 **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff TRACIE WILSON ("Plaintiff") brings this Class Action Complaint ("Complaint") against Defendants HARVARD PILGRIM HELATH CARE, INC. and POINT32HEALTH, INC. ("HPHC" and "Point32" or, collectively, "Defendants") as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to her own actions and her counsels' investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This Class Action arises from a recent cyberattack resulting in a data breach of sensitive information in the possession and custody and/or control of the Defendants (the "Data Breach").

2. Harvard Pilgrim is a health insurance provider that operates in the New England region. Point32 is Harvard Pilgrim's parent company and was created as a result of a merger between Harvard Pilgrim and Tufts Health Plan.

3. The Data Breach resulted in the unauthorized disclosure, exfiltration, and theft of current and former customers' highly personal information, including names, Social Security numbers, dates of birth, phone numbers, addresses, provider taxpayer identification numbers, ("personal identifying

information" or "PII"), and health insurance account information and clinical information ("protected health information" or "PHI"). Plaintiff refers to both PII and PHI collectively as "Sensitive Information."

4. On information and belief, the Data Breach occurred between March 28, 2023, and April 17, 2023. Defendants did not become aware of suspicious activity on their network until April 17, 2023, allowing cybercriminals unfettered access to Plaintiff and the Class's Sensitive Information for *twenty* days.

5. On May 24, 2023, Defendants finally began notifying Class Members about the widespread Data Breach ("Breach Notice") through Breach Notice Letters and their website.[1] An example of the Breach Notice Letter is attached as Exhibit A. Defendants waited over a month before informing Plaintiff and Class Members about the breach, even though Plaintiff and approximately 2.5 million[2] Class Members had their most sensitive personal information accessed, exfiltrated, and stolen,[3] causing them to suffer ascertainable losses in the form of the loss of the benefit of their bargain and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

6. Defendants' Breach Notice obfuscated the nature of the breach and the threat it posted—refusing to tell their customers how many people were impacted, how the breach happened, or why it took Defendants over a month to begin notifying victims that hackers had gained access to highly private Sensitive Information.

7. Defendants' failure to timely detect and report the Data Breach made their customers vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their Sensitive Information.

---

[1] Notice of Data Security Incident, HPHC, https://www.harvardpilgrim.org/data-security-incident/ (last visited June 6, 2023)

[2] HPHC Reports Data Breach Following Ransomware attack, JD Supra, https://www.jdsupra.com/legalnews/harvard-pilgrim-health-care-reports-4827511/#:~:text=On%20May%2024%2C%202023%2C%20Harvard,patients'%20confidential%20information%20being%20leaked (last visited June 6, 2023)

8. Defendants knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII and PHI misuse.

9. In failing to adequately protect Plaintiff's and the Class's Sensitive Information, failing to adequately notify them about the breach, and by obfuscating the nature of the breach, Defendants violated state and federal law and harmed an unknown number of their current and former customers.

10. Plaintiff and members of the proposed Class are victims of Defendants' negligence and inadequate cyber security measures. Specifically, Plaintiff and members of the proposed Class trusted Defendants with their Sensitive Information. But Defendants betrayed that trust. Defendants failed to properly use up-to-date security practices to prevent the Data Breach.

11. Plaintiff Tracie Wilson is a Data Breach victim.

12. Accordingly, Plaintiff, on her own behalf and on behalf of a class of similarly situated individuals, brings this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendants' possession.

PARTIES

13. Plaintiff, Tracie Wilson, is a natural person and citizen of New Hampshire, where she intends to remain. Plaintiff Wilson is a Data Breach victim, receiving the Breach Notice on approximately May 2, 2023.

14. Defendant, Point32 is a Massachusetts corporation, with its principal place of business at 1 Wellness Way, Canton, MA 02021.

15. Defendant, HPHC, is a Massachusetts corporation, with its principal place of business at 1 Wellness Way, Canton, MA 02021.

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000,

exclusive of interest and costs, there are more than 100 members in the proposed class. Plaintiff and Defendants are citizens of different states.

17. This Court has personal jurisdiction over Defendants because Defendants maintain their principal place of business this District and does substantial business in this District.

18. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claim occurred in this District.

STATEMENT OF FACTS

Point32 and HPHC

19. Point32 is "a family of companies" that includes but is not limited to HPHC and Tufts Health Plan[4], with the name Point32 serving as "[the company's] corporate name". [5]

20. HPHC is a nonprofit healthcare company in Massachusetts that provides "high- quality and affordable health care" to their customers. Together, Defendants provide health insurance "to more than 3 million customers in New England and beyond".[6] Defendants have a total annual revenue of $9.4 billion.[7]

21. As part of their business, Defendants receive and maintain the Sensitive Information of thousands of current and former customers. In doing so, Defendants implicitly promise to safeguard their Sensitive Information.

22. In collecting and maintaining their current and former customers' Sensitive Information, Defendants agreed that they would safeguard the data in accordance with their internal policies, state law, and federal law. After all, Plaintiff and Class Members themselves took reasonable steps to secure their Sensitive Information

[4] Our Family of Companies, Point32 Health, https://www.point32health.org/about-us/our-family-of-companies/ (last visited June 6, 2023).
[5] *Id*.
[6] About Us, HPHC, https://www.harvardpilgrim.org/public/about-us (last visited Mar. 15, 2023).
[7] Point32, Zippia, https://www.zoominfo.com/c/point32health-inc/558709403 (last visited June 6, 2023).

23. Indeed, Defendants promise in their Privacy Policy that they are "required by law to maintain the privacy of your information" and does so by using "privacy and security policies for safeguarding, using, and disclosing information in compliance with applicable state and federal laws." [8]

24. Defendants boast that, to ensure the privacy of their customers' PII and PHI information, they require "all employees [to] complete annual privacy and security training" and that "access to your information is limited to employees who require it to do their job."[9]

> you. We are required by law to maintain the privacy of your information. To support this, Harvard Pilgrim has privacy and security policies for safeguarding, using, and disclosing information in compliance with applicable state and federal laws. All employees must complete annual privacy and security training, and access to your information is limited to employees who require it to do their job. Harvard Pilgrim also requires its business partners who assist with administering health care coverage to you on our behalf to protect your information in accordance with applicable laws.

25. Point32 has an additional privacy policy on its website, stating that "[w]hen we link to the sites of Harvard Pilgrim Health Care or Tufts Health Plan business associates where personal health information (PHI) is collected on our behalf, those sites are required to safeguard information in accordance with HIPAA."[10]

26. Despite recognizing their duty to do so, on information and belief, Defendants have not implemented reasonably cybersecurity safeguards or policies to protect their customers' Sensitive Information or supervised their IT or data security agents and employees to prevent, detect, and stop breaches of their systems. As a result, Defendants leave significant vulnerabilities in their system for cybercriminals to exploit and gain access to customers' Sensitive Information.

---

[8] Harvard Pilgrim Notice of Policy Practices, https://www.uhcsr.com/media/d3579672-cc79-4b4b-8567-c6eb980416ba (last visited June 6, 2023).
[9] *Id.*
[10] Privacy & Security, Point32 Health, https://www.point32health.org/privacy-policy/ (last visited June 6, 2023).

The Data Breach

27. Plaintiff has been a member of Harvard Pilgrim Health Center since 2019. As a condition of receiving HPHC's services, Plaintiff provided HPHC with her Sensitive Information, including but not limited to her name, Social Security number, dates of birth, phone number, address, provider taxpayer identification number, health insurance information, and clinical treatment information. Defendants used that Sensitive Information to facilitate services to Plaintiff and required Plaintiff to provide that Sensitive Information to obtain their services.

28. On information and belief, Defendants collect and maintain customers' Sensitive Information in their computer systems.

29. In collecting and maintaining Sensitive Information, Defendants implicitly agree that they would safeguard the data using reasonable means according to their internal policy, as well as state and federal law.

30. According to the Breach Notice, Defendants "discovered a cybersecurity ransomware incident that impacted systems that support Harvard Pilgrim Health Care Commercial and Medicare Advantage Strike plans," on April 17, 2023, and that "the investigation identified signs that data was copied and taken from our Harvard Pilgrim systems from March 28, 2023, to April 17, 2023." Ex. A.

31. In other words, Defendants investigation revealed that cybercriminals had had unfettered access to Plaintiff's and the Class's Sensitive Information for *twenty* days before Defendants finally discovered of the Breach.

32. Defendants' cyber and data security systems were completely inadequate and allowed cybercriminals to obtain files containing a treasure trove of millions of its customers' highly private Sensitive Information.

33. Additionally, Defendants admitted that Sensitive Information was *actually stolen*, stating that there were "signs that **data was copied and taken**". Ex.A.

34. On or around May 24, 2023–over a month after the Breach first occurred– Defendants finally notified Plaintiff and Class Members about the Data Breach.

35. Despite its duties and alleged commitments to safeguard Sensitive Information, Defendants did not in fact follow industry standard practices in securing customers' Sensitive Information, as evidenced by the Data Breach.

36. In response to the Data Breach, Defendants contend that they have or will be " tak[ing] steps to implement additional data security enhancements and safeguards to better protect against similar events" Ex. A. Although Defendants fail to expand on what these alleged "steps" are, such safeguards and training should have been in place before the Data Breach.

37. Through their Breach Notice, Defendants also recognized the actual imminent harm and injury that flowed from the Data Breach, so they encouraged breach victims to take steps "to help protect [victims'] personal information" including placing "an initial or extended fraud alert" as well as a "credit freeze on a credit report". Ex. A.

38. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff's and the Class's Sensitive Information. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff's and the Class's financial accounts.

39. On information and belief, Defendants have offered some amount of complimentary credit monitoring services to victims, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the breach involves Sensitive Information that cannot be changed, such as Social Security numbers.

40. Even with several months' worth of credit monitoring services, the risk of identity theft and unauthorized use of Plaintiff's and Class Members' Sensitive Information is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

41. On information and belief, Defendants failed to adequately train and supervise their IT and data security agents and employees on reasonable cybersecurity protocols or implement reasonable security measures, causing Defendants to lose control over their customers' Sensitive Information. Defendants'

negligence is evidenced by their failure to prevent the Data Breach and stop cybercriminals from accessing the Sensitive Information.

The Data Breach was a Foreseeable Risk of which Defendants were on Notice.

42. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare or healthcare adjacent industries preceding the date of the breach.

43. In light of recent high profile data breaches at other healthcare partners and provider companies, Defendants knew or should have known that their electronic records and customers' Sensitive Information would be targeted by cybercriminals.

44. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[11] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[12]

45. Indeed, cyberattacks against the healthcare industry have become increasingly common for over ten years, with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[13]

---

[11] 2021 Data Breach Annual Report, ITRC, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf (last visited June 5, 2023).

[12] *Id*.

[13] Gordon M. Snow Statement, FBI https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector (last visited March 13, 2023).

46. Cyberattacks on medical systems and healthcare partner and provider companies like Defendants have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[14]

47. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendants' industry, including Point32 and HPHC.

Plaintiff Wilson's Experience

48. Plaintiff has been a member of Harvard Pilgrim Health Center's Medicare Advantage Stride since 2019. As a condition of receiving HPHC's services, Plaintiff provided Defendants with her Sensitive Information, including but not limited to her name, Social Security number, dates of birth, phone number, address, provider taxpayer identification number, health insurance information, and clinical treatment information. Defendants used that Sensitive Information to facilitate their services to Plaintiff and required Plaintiff to provide that Sensitive Information to obtain Defendants' services.

49. Plaintiff provided her Sensitive Information to Defendants and trusted that they would use reasonable measures to protect it according to their internal policies and state and federal law.

50. Plaintiff reasonably believed that a portion of the funds she paid Defendants for their health insurance services would be used to provide adequate data security for her Sensitive Information.

---

[14] Secret Service Warn of Targeted, Law360, https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited March 13, 2023).

51. Defendants deprived Plaintiff of the earliest opportunity to guard herself against the Data Breach's effects by failing to notify her about it for over a month.

52. Indeed, Plaintiff has experienced an increase in spam texts and phone calls since the Data Breach, suggesting that her Sensitive Information has been placed in the hands of cybercriminals.

53. Plaintiff does not recall ever learning that her Sensitive Information was compromised in a data breach incident, other than the breach at issue in this case.

54. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

55. Plaintiff has and will spend considerable time and effort monitoring her accounts to protect herself from additional identity theft. Plaintiff fears for her personal financial security and uncertainty over what Sensitive Information was exposed in the Data Breach.

56. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

57. Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff's Sensitive Information—a form of intangible property that Plaintiff entrusted to Defendants, which was compromised in and as a result of the Data Breach.

58. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Sensitive Information being placed in the hands of unauthorized third parties and possibly criminals.

59. Plaintiff has a continuing interest in ensuring that her Sensitive Information, which, upon information and belief, remains backed up in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

60. Plaintiff and members of the proposed Class have suffered injury from the misuse of their Sensitive Information that can be directly traced to Defendants.

61. As a result of Defendants' failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their Sensitive Information is used;

b. The diminution in value of their Sensitive Information;

c. The compromise and continuing publication of their Sensitive Information;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen Sensitive Information; and

h. The continued risk to their Sensitive Information, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake the appropriate measures to protect the Sensitive Information in their possession.

62. Stolen Sensitive Information is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII alone can be worth up to $1,000.00 depending on the type of information obtained.

63. The value of Plaintiff's and the Class's Sensitive Information on the black market is considerable. Stolen Sensitive Information trades on the black market for years, and criminals frequently post stolen Sensitive Information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

64. It can take victims years to spot identity theft, giving criminals plenty of time to use that information for cash.

65. One such example of criminals using Sensitive Information for profit is the development of "Fullz" packages.

66. Cyber-criminals can cross-reference two sources of Sensitive Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

67. The development of "Fullz" packages means that stolen Sensitive Information from the Data Breach can easily be used to link and identify it to Plaintiff and the proposed Class' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Sensitive Information stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and the Class's stolen Sensitive Information is being misused, and that such misuse is fairly traceable to the Data Breach.

68. Defendants disclosed the Sensitive Information of Plaintiff and the Class for criminals to use in the conduct of criminal activity. Specifically, Defendants opened up, disclosed, and exposed the Sensitive Information of Plaintiff and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen Sensitive Information.

69. Defendants' failure to properly notify Plaintiff and members of the Class of the Data Breach exacerbated Plaintiff's and the Class's injury by depriving them of the earliest ability to take appropriate measures to protect their Sensitive Information and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendants failed to adhere to FTC guidelines.

70. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued

numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of Sensitive Information.

71. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the sensitive consumer information that it keeps;

b. properly dispose of Sensitive Information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

72. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

73. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

74. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

75. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' Sensitive Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendants Violated HIPAA

76. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients', or in this case, customers', medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information. [15]

77. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII and PHI is properly maintained.[16]

78. The Data Breach itself resulted from a combination of inadequacies showing Defendants' failure to comply with safeguards mandated by HIPAA. Defendants' security failures include, but are not limited to:

a. Failing to ensure the confidentiality and integrity of electronic PHI that they create, receive, maintain and transmit in violation of 45 C.F.R. § 164.306(a)(1);

b. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

---

[15] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, inter alia: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

[16] *See* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

c. Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

d. Failing to ensure compliance with HIPAA security standards by Defendants in violation of 45 C.F.R. § 164.306(a)(4);

e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

79. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrate Defendants failed to comply with safeguards mandated by HIPAA regulations.

Defendants Fail to Comply with Industry Standards

80. As noted above, experts studying cyber security routinely identify entities in possession of PII and PHI as being particularly vulnerable to cyberattacks because of the value of the Sensitive Information which they collect and maintain.

81. Several best practices have been identified that a minimum should be implemented by employers in possession of PII and PHI, like Defendants, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendants failed to follow these industry best practices, including a failure to implement multi-factor authentication.

82. Other best cybersecurity practices that are standard for employers include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendants failed to follow these cybersecurity best practices, including failure to train staff.

83. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center

for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

84. These foregoing frameworks are existing and applicable industry standards for a company's obligation to provide adequate data security for its customers. Upon information and belief, Defendants failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

CLASS ACTION ALLEGATIONS

85. Plaintiff sues on behalf of herself and the proposed Class , defined as follows, pursuant to Federal Rule of Civil Procedure 23(b)(2) and (b)(3):

> All individuals residing in the United States whose Sensitive Information was compromised in the Point32 and HPHC Data Breach including all those who received notice of the breach.

86. Excluded from the Class are Defendants, their agents, affiliates, parents, subsidiaries, any entity in which Defendants have a controlling interest, any of Defendants' officers or directors, any successors, and any Judge who adjudicates this case, including their staff and immediate family.

87. Plaintiff reserves the right to amend the class definition.

88. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

a. **Numerosity**. Plaintiff is representative of the Class, consisting of 3.55 million individuals, far too many to join in a single action;

b. **Ascertainability**. Members of the Class are readily identifiable from information in Defendants' possession, custody, and control;

c. **Typicality**. Plaintiff's claims are typical of class claims as each arises from the same Data Breach, the same alleged violations by Defendants, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's interests. Her interests do not conflict with the Class's interests, and she has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Commonality**. Plaintiff's and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for the Class. Indeed, it will be necessary to answer the following questions:

   i. Whether Defendants had a duty to use reasonable care in safeguarding Plaintiff's and the Class's Sensitive Information;

   ii. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

   iii. Whether Defendants were negligent in maintaining, protecting, and securing Sensitive Information;

   iv. Whether Defendants breached contract promises to safeguard Plaintiff's and the Class's Sensitive Information;

   v. Whether Defendants took reasonable measures to determine the extent of the Data Breach after discovering it;

   vi. Whether Defendants' Breach Notice was reasonable;

   vii. Whether the Data Breach caused Plaintiff's and the Class's injuries;

viii. What the proper damages measure is; and

ix. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

89. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

90. Plaintiff realleges all previous paragraphs as if fully set forth below.

91. Plaintiff and members of the Class entrusted their Sensitive Information to Defendants. Defendants owed to Plaintiff and the Class a duty to exercise reasonable care in handling and using the Sensitive Information in their care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

92. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and the Class's Sensitive Information.

93. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers' Sensitive Information. The FTC publications and orders promulgated pursuant to the FTC Act

also form part of the basis of Defendants' duty to protect Plaintiff's and the members of the Class's Sensitive Information.

94. Defendants breached their duties to Plaintiff and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Sensitive Information.

95. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and their customers, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendants were in a position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach.

96. Defendants' duty to use reasonable security measures under HIPAA required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

97. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential Sensitive Information.

98. Defendants violated their duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and the Class's Sensitive Information and not complying with applicable industry standards as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of Sensitive Information

Defendants collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

99. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

100. Defendants violated their duty under HIPAA by failing to use reasonable measures to protect their PHI and by not complying with applicable regulations detailed supra. Here too, Defendants' conduct was particularly unreasonable given the nature and amount of Sensitive Information Defendants collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

101. Defendants owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Defendants' failure to adequately safeguard their Sensitive Information in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that Sensitive Information —just like the Data Breach that ultimately came to pass. Defendants acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and the Class's Sensitive Information by disclosing and providing access to this information to unauthorized third parties and by failing to properly supervise both the way the Sensitive Information was stored, used, and exchanged, and those in their employment who were responsible for making that happen.

102. Defendants owed to Plaintiff and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their Sensitive Information. Defendants also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and the Class to take appropriate measures to protect their Sensitive Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

103. Defendants owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendants knew or should have known would suffer injury-in-fact from Defendants' inadequate security protocols. Defendants actively sought and obtained Plaintiff's and the Class's Sensitive Information.

104. The risk that unauthorized persons would attempt to gain access to the Sensitive Information and misuse it was foreseeable. Given that Defendants hold vast amounts of Sensitive Information, it was inevitable that unauthorized individuals would attempt to access Defendants' databases containing the Sensitive Information —whether by malware or otherwise.

105. Sensitive Information is highly valuable, and Defendants knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Sensitive Information of Plaintiff and the Class and the importance of exercising reasonable care in handling it.

106. Defendants breached their duties by failing to exercise reasonable care in supervising their employees, agents, contractors, vendors, and suppliers, and in handling and securing the Sensitive Information of Plaintiff and the Class which actually and proximately

caused the Data Breach and Plaintiff's and the Class's injury. Defendants further breached their duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and members of the Class's injuries-in-fact. As a direct and traceable result of Defendants' negligence and/or negligent supervision, Plaintiff and the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

107. Defendants' breach of their common-law duties to exercise reasonable care and their failures and negligence actually and proximately caused Plaintiff and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their Sensitive Information by criminals, improper disclosure of their Sensitive Information, lost benefit of their bargain, lost value of their Sensitive Information, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendants' negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
Breach of an Implied Contract
(On Behalf of Plaintiff and the Class)

108. Plaintiff realleges all previous paragraphs as if fully set forth below.

109. Plaintiff and the Class delivered their Sensitive Information to Defendants as part of the process of obtaining services provided by Defendants.

110. Plaintiff and Class Members entered into implied contracts with Defendants under which Defendants agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class Members if and when their data had been breached and

compromised. Each such contractual relationship imposed on Defendants an implied covenant of good faith and fair dealing by which Defendants were required to perform their obligations and manage Plaintiff's and Class Members' data in a manner which comported with the reasonable expectations of privacy and protection attendant to entrusting such data to Defendants.

111. In providing their Sensitive Information, Plaintiff and Class Members entered into an implied contract with Defendants whereby Defendants, in receiving such data, became obligated to reasonably safeguard Plaintiff's and the other Class Members' Sensitive Information.

112. In delivering their Sensitive Information to Defendants, Plaintiff and Class Members intended and understood that Defendants would adequately safeguard that data.

113. Plaintiff and the Class Members would not have entrusted their Sensitive Information to Defendants in the absence of such an implied contract.

114. Defendants accepted possession of Plaintiff's and Class Members' Sensitive Information.

115. Had Defendants disclosed to Plaintiff and Class Members that Defendants did not have adequate computer systems and security practices to secure customers' Sensitive Information, Plaintiff and members of the Class would not have provided their Sensitive Information to Defendants.

116. Defendants recognized that customers' Sensitive Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and Class Members.

117. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendants.

118. Defendants breached the implied contract with Plaintiff and Class Members by failing to take reasonable measures to safeguard their data.

119. Defendants breached the implied contract with Plaintiff and Class Members by failing to promptly notify them of the access to and exfiltration of their Sensitive Information.

120. As a direct and proximate result of the breach of the contractual duties, Plaintiff and Class Members have suffered actual, concrete, and imminent injuries. The injuries suffered by Plaintiff and the Class Members include: (a) the invasion of privacy; (b) the compromise, disclosure, theft, and unauthorized use of Plaintiff's and Class Members' Sensitive Information; (c) economic costs associated with the time spent to detect and prevent identity theft, including loss of productivity; (d) monetary costs associated with the detection and prevention of identity theft; (e) economic costs, including time and money, related to incidents of actual identity theft; (f) the emotional distress, fear, anxiety, nuisance and annoyance of dealing related to the theft and compromise of their Sensitive Information; (g) the diminution in the value of the services bargained for as Plaintiff and Class Members were deprived of the data protection and security that Defendants promised when Plaintiff and the proposed class entrusted Defendants with their Sensitive Information; and (h) the continued and substantial risk to Plaintiff's and Class Members' Sensitive Information, which remains in the Defendants' possession with inadequate measures to protect Plaintiff's and Class Members' Sensitive Information.

COUNT III
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

121. Plaintiff realleges all previous paragraphs as if fully set forth below.

122. This claim is pleaded in the alternative to the breach of implied contractual duty claim.

123. Plaintiff and members of the Class conferred a benefit upon Defendants in providing Sensitive Information to Defendants.

124. Defendants appreciated or had knowledge of the benefits conferred upon them by Plaintiff and the Class. Defendants also benefited from the receipt of Plaintiff's and the Class's Sensitive Information, as this was used to facilitate services and goods they sold to Plaintiff and the Class.

125. Under principles of equity and good conscience, Defendants should not be permitted to retain the full value of Plaintiff and the Class's Sensitive Information because Defendants failed to adequately protect their Sensitive Information. Plaintiff and the proposed Class would not have provided their Sensitive Information to Defendants had they known Defendants would not adequately protect their Sensitive Information.

126. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiff and members of the Class all unlawful or inequitable proceeds received by them because of their misconduct and Data Breach.

COUNT IV
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

127. Plaintiff realleges all previous paragraphs as if fully set forth below.

128. As a condition of obtaining services from Defendants, Plaintiff and Class members gave Defendants their Sensitive Information in confidence, believing that Defendants would protect that information. Plaintiffs and Class members would not have provided Defendants with this information had they known it would not be adequately protected. Defendants' acceptance and storage of Plaintiffs' and Class members' Sensitive Information

created a fiduciary relationship between Defendants and Plaintiffs and Class members. In light of this relationship, Defendants must act primarily for the benefit of their customers, which includes safeguarding and protecting Plaintiffs' and Class members' Sensitive Information.

129. Defendants have a fiduciary duty to act for the benefit of Plaintiffs and Class members upon matters within the scope of their relationship. Defendants breached that duty by failing to properly protect the integrity of the system containing Plaintiffs' and Class members' Sensitive Information, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Plaintiffs' and Class members' Sensitive Information that they collected.

130. As a direct and proximate result of Defendants' breach of their fiduciary duties, Plaintiffs and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise, publication, and theft of their Sensitive Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their Sensitive Information; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their Sensitive Information which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the Sensitive Information compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

PRAYER FOR RELIEF

Plaintiff and the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representatives, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendants from further deceptive practices and making untrue statements about the Data Breach and the stolen Sensitive Information;

E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

Dated: June 7, 2023.

Respectfully submitted,

By: */s/ Robert Bonsignore*

TURKE & STRAUSS LLP
Samuel J. Strauss
Raina Borrelli
613 Williamson Street, Suite 201
Madison, Wisconsin 53703
Telephone: (608) 237-1775
Facsimile: (608) 509-4423
sam@turkestrauss.com
raina@turkestrauss.com

J. Gerard Stranch, IV (*Pro Hac Vice* forthcoming)
Andrew E. Mize (*Pro Hac Vice* forthcoming)
STRANCH, JENNINGS & GARVEY, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
(615) 254-8801
(615) 255-5419 (facsimile)
gstranch@stranchlaw.com
amize@stranchlaw.com

Robert J. Bonsignore, Esq. (BBO #547880)
Melanie Porter (CA #253500)**
23 Forest St.
Medford, Massachusetts 02155
Mobile: (781) 354-1800
Office: (781) 350-0000
Facsimile: (702) 983-8673
Email: rbonsignore@classactions.us
Email: melanie@classactions.us

Lynn A. Toops (*Pro Hac Vice* forthcoming)
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, Indiana 46204
(317) 636-6481
ltoops@cohenandmalad.com

Attorneys for Plaintiff and Proposed Class